

**Fermilab  
FY2003 Self-assessment  
Process Assessment Report  
For  
Technical Division**

**15-Jan-2003**

Division/Section performing assessment

Technical Division

Name of organization that owns assessed process

Technical Division

Organization Strategy

With the increase in awareness of security issues, cyber security has become a very high priority. It is the Division's policy to follow the policies defined by the Directorate and the Computing Division in this matter.

It is the Computing & Information Systems Department (CIS) which is responsible for ensuring that the Division manages its information systems securely.

Names of Personnel on Assessment team

Jamie Blowers, Quality Assurance Officer

Name of process assessed

Security of Information Systems in Technical Division

Brief description of process to be assessed

Information Systems Security, a.k.a. Cyber security, is the work of managing computing and information systems in such a way to prevent loss of data while maximizing up-time. Loss of data could come in many ways, including hardware/software failures and through the work of outside "hackers".

Are metrics associated with this process? If so, what are they?

There are no contractual or internal metrics for this process.

What are the names of the procedures associated with this process?

Fermilab Policy on Computing  
Cyber Security Program Plan (CSPP)  
TD policy TS-1020 Computer Security

Are these procedures being followed? Are they current?

The first two procedures listed above are being followed and are current. It should be noted that, for security reasons, the auditor was not able to see the CSPP, but nonetheless believes it to be current.

It was acknowledged that TS-1020 is out of date, and should be updated.

Describe the methodology used to assess this process.

The methodology followed standard auditing practices. The Lead Auditor created a checklist (see attached) and sent it to the auditees approximately one week prior to the audit. The audit consisted of interviews with those involved in cyber security. The interviews were based on the topics outlined in the checklist.

Results of the assessment:

Overall the results of the assessment are **good**. Most areas assessed are fully compliant with the Fermilab Policy on Computing. Most issues that need to be addressed are centered around documenting work practices, and not problems with the work practices themselves.

Specifically, the work of upgrading to the FERMI domain (i.e. the strengthened realm) is central to the current security policies for the Laboratory. This work in the Division is proceeding on schedule, and by the end of January 2003, it should be complete for all user workstations. By completing this task, the Division will be fully complying with the security policies set by the Directorate and the Computing Division regarding the use of passwords and the upgrade to the strengthened realm.

Further details on the results of the assessment are documented in the attached checklist.

Identified opportunities for improvement

The following items were identified as opportunities for improvement:

1. TD policy TS-1020 should be updated to reflect current policy and work practices.
2. The methods of doing backups/restores should be documented and published.
3. A 'disaster recovery plan' should be defined and documented.
4. The methods used to protect web content needs to be reviewed and defined

appropriately (e.g. the use of network usernames/passwords to authenticate over the internet should be reviewed).

5. Responsibility should be defined (i.e. names assigned) for people responsible for managing web content that is intended for the public.
6. Implement a mechanism for tracking updates/patches applied to systems which do not have internal tracking mechanisms in place (e.g. MS SQL Server).

#### Schedule for implementation of improvements

The schedule for implementation is being worked out.

#### Status of improvements from previous assessment

N/A

#### Attachments (supporting data, worksheets, reports, etc.)

The following attachments have been incorporated into this report:

Checklist – the checklist used to conduct the assessment.

Backup/restore records – records provided as evidence of the backup/restore system.

Fermilab Policy on Computing – the document published by Computing Division which summarizes the policies related to computing.

DOE N 205.1 – the DOE contractual notice on Unclassified Cyber Security Program.

## TD-2003-02 Information Systems Security - Audit Checklist

<i>Reference</i>	<i>Criteria</i>	<i>Results</i>			<i>Comments</i>
		<i>Fully Sat</i>	<i>Minor Issue</i>	<i>Major Issue</i>	
Fermilab Policy on Computing	Proper use and protection of passwords - is there a Lab-wide policy document? - is there a TD policy document? - Prime Contract: N 205.1, N205.3, G 205.3-1 - “Cyber Security Program Plan (CSPP)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	- Fermilab has a CSPP. It is not available publicly (or to the auditor without prior permission). This document contains details regarding the policies regarding the proper use and protection of passwords. The policies are enforced through the “strengthened realm” – i.e. the specifics of how passwords are created and managed are forced by joining the FERMI domain. The document is currently version 5.1 dated 06-Aug-2002. - TD does not have a formal policy document on this topic. Conversations are taking place about this, but it is not expected that any formal policy will be documented and published, as this could create a security risk. - TD has not been formally assessed against the CSPP.
Fermilab Policy on Computing/ TD policy TS-1020	Physical protection of computers - Is TS-1020 current?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	- No one has ever stolen a PC from the TD. - It was acknowledged that not all PCs are physically locked down. It was estimated that 70% are secured (either in an office with a lock or with a tie-down). - <i>It was acknowledged that TS-1020 is out of date, and that it should be updated (should include portables).</i>
Fermilab Policy on Computing	Regular backup of important data - details from page 8 of computing policy	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	- TD has ~ 1 Terabyte of data requiring backup. - TD does everything required in the policy except publish how backups/restores are done, and <i>it was acknowledged that it would be a good idea to document and publish this.</i> - <i>It was acknowledged that TD should define and document a ‘disaster recovery plan’.</i>

## TD-2003-02 Information Systems Security - Audit Checklist

<i>Reference</i>	<i>Criteria</i>	<i>Results</i>			<i>Comments</i>
		<i>Fully Sat</i>	<i>Minor Issue</i>	<i>Major Issue</i>	
Fermilab Policy on Computing	Incident reporting	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	- TD fully complies with the requirements. - CIS is working on a checklist which will be used to do an assessment when issues are identified; this checklist should be finished and published.
Fermilab Policy on Computing	Restricted central services: - routing/bridging - tunneling - all offsite connections (except modems) - assignment of IP and DECNET host names - DNS zone mastering and all externally-reachable DNS service - NTP time service at stratum 1 - NNTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TD does not do any of these things and so fully complies with the policy.
Fermilab Policy on Computing	System managers - are all CIS employees system managers? - does TD have any "critical system domains"?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	- All CIS employees are System Managers. - Levels of administration are appropriately managed (e.g. privileges of system administration are given when needed, and at appropriate levels as required to do the work). - TD does not have any critical system domains.
Fermilab Policy on Computing	Access control/strengthened realms - what does all this mean and how is it applied within TD?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	- At the time of the assessment, TD was less than 15 PC's from having all user computers being converted to the FERMI domain. This will be completed by the end of January. - TD servers will be converted later.
Fermilab Policy on Computing	Public versus restricted access (page 13) - how has TD handled this topic?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	- This is mostly handled through ACL and IP address restrictions. Some is handled using NT permissions, which prompt for username/password. <i>It is acknowledged that this should be looked at in more detail so that it is being appropriately managed.</i>

## TD-2003-02 Information Systems Security - Audit Checklist

<i>Reference</i>	<i>Criteria</i>	<i>Results</i>			<i>Comments</i>
		<i>Fully Sat</i>	<i>Minor Issue</i>	<i>Major Issue</i>	
Fermilab Policy on Computing	Material intended for the Lay or Scientific public - how has TD handled this topic?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	- Naming a person for each publicly-oriented web page is an open issue. It is likely that a team will be assembled which will be responsible for managing the publicly-oriented web pages.
Fermilab Policy on Computing	Semi-official/public web pages - disclaimer required on all pages	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	All TD web pages have the disclaimer.
Fermilab Policy on Computing	Cookies - do we use them? - how is this tracked?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TD does not use cookies on web pages that are intended for the public.
Fermilab Policy on Computing	Use of computers in systems that protect...(page 16) - do we have any of this in TD (e.g. IB1, MS)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	There are no systems in the TD which use computers to protect people, property, or the environment. <b><i>John is going to get back to me regarding IB1.</i></b>
CIAC/CERT DOE N 205.1 (CRD #13)	How do we handle the CIAC/CERT bulletins? - e.g. SQL Server vulnerability (N-003 <a href="http://ciac.llnl.gov/ciac/bulletins/n-003.shtml">http://ciac.llnl.gov/ciac/bulletins/n-003.shtml</a> )	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	- CIS personnel receive e-mails regarding bulletins and alerts. CIS also periodically checks forums for special alerts. - When alerts are known, the appropriate fixes/patches are applied very quickly. - It was noted that Microsoft SQL Server does not have an internal mechanism for tracking patches or updates. <i>For systems like this, another mechanism should be employed to keep track of patches/updates (e.g. a log file).</i>
DOE N 205.1 (CRD #14)	Training - Have CIS personnel received training on cyber security?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	- The TD point-person for cyber-security has received some formal training in cyber-security (from outside sources).

**Backup Exec - [Activity Monitor]**

File View Admin Network Select Jobs Tools Window Help

Backup Restore

## Scheduled, Active, and Completed Jobs

Class	Job Name	Device Name	Job Type	Job Status	Percent ...	Start Time	Elapsed Time	Byte Count
Scheduled	TDserver User Data	QUANTUM 5	Backup	On Hold		1/25/2003 11:10 AM		
Scheduled	DCS	QUANTUM 4	Backup	Scheduled		1/25/2003 4:02 AM		
Scheduled	TDserver Op Sys	QUANTUM 5	Backup	On Hold		1/25/2003 3:00 AM		
Scheduled	DCS incremental	QUANTUM 5	Backup	Scheduled		1/22/2003 3:05 AM		
Scheduled	TD Calendar Full	QUANTUM 4	Backup	Scheduled		1/22/2003 2:09 AM		
Scheduled	TDserver Incremental	QUANTUM 5	Backup	Scheduled		1/21/2003 11:55 PM		
Active	andreev's bookmarks		Restore	Loading Media		1/21/2003 10:17 AM	1:33:25	0
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/21/2003 3:05 AM	1:15:44	9,402,995,662
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/21/2003 2:09 AM	0:08:20	169,903,925
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/20/2003 11:55 PM	1:17:11	5,536,108,912
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/20/2003 3:05 AM	1:16:39	9,402,995,662
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/20/2003 2:09 AM	0:05:57	169,903,925
Completed	TDserver User Data	QUANTUM 5	Backup	Successful	100%	1/18/2003 11:48 PM	16:19:24	500,597,966,341
Completed	TDserver Op Sys	QUANTUM 5	Backup	Failed	Unknown	1/18/2003 4:28 PM	5:56:55	88,245,048,457
Completed	DCS	QUANTUM 4	Backup	Successful	100%	1/18/2003 4:02 AM	1:17:40	9,402,995,662
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/17/2003 11:55 PM	1:31:28	18,226,623,135
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/17/2003 2:49 PM	0:10:20	171,011,821
Completed	TD Calendar Full	QUANTUM 4	Backup	Failed	Unknown	1/17/2003 2:09 AM	0:52:33	168,065,329
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/16/2003 11:55 PM	9:49:01	25,986,760,999
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/16/2003 3:05 AM	24:40:25	9,398,343,522
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/16/2003 2:09 AM	0:07:32	169,480,049
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/15/2003 11:55 PM	1:41:02	20,221,084,900
Completed	Cleaning 0265	QUANTUM 4	Cleaning	Successful	100%	1/15/2003 7:23 AM	0:10:01	0
Completed	Cleaning 0264	QUANTUM 5	Cleaning	Successful	100%	1/15/2003 7:23 AM	1:49:22	0
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/15/2003 7:15 AM	1:45:32	20,079,351,606
Completed	Device Job 0001	OVERLAND 1	Inventory	Completed	100%	1/15/2003 7:14 AM	0:01:25	
Completed	DCS incremental		Backup	Canceled	N/A	1/15/2003 3:05 AM	4:01:13	0
Completed	Cleaning 0263		Cleaning	Canceled	N/A	1/15/2003 2:20 AM	0:02:55	0
Completed	TD Calendar Full	QUANTUM 4	Backup	Failed	Unknown	1/15/2003 2:09 AM	0:12:27	0
Completed	TDserver Incremental		Backup	Canceled	N/A	1/14/2003 11:55 PM	2:27:41	0

Backup Selections Restore Selections Job Definitions **Activity Monitor** Devices Media Reports Alerts

Ready TDARCHIVE

Start SGMon Backup Exec - [Activit...

11:51 AM

**Backup Exec - [Activity Monitor]**

File View Admin Network Select Jobs Tools Window Help

Backup Restore

## Scheduled, Active, and Completed Jobs

Class	Job Name	Device Name	Job Type	Job Status	Percent ...	Start Time	Elapsed Time	Byte Count
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/17/2003 2:49 PM	0:10:20	171,011,821
Completed	TD Calendar Full	QUANTUM 4	Backup	Failed	Unknown	1/17/2003 2:09 AM	0:52:33	168,065,329
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/16/2003 11:55 PM	9:49:01	25,986,760,999
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/16/2003 3:05 AM	24:40:25	9,398,343,522
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/16/2003 2:09 AM	0:07:32	169,480,049
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/15/2003 11:55 PM	1:41:02	20,221,084,900
Completed	Cleaning 0265	QUANTUM 4	Cleaning	Successful	100%	1/15/2003 7:23 AM	0:10:01	0
Completed	Cleaning 0264	QUANTUM 5	Cleaning	Successful	100%	1/15/2003 7:23 AM	1:49:22	0
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/15/2003 7:15 AM	1:45:32	20,079,351,606
Completed	Device Job 0001	OVERLAND 1	Inventory	Completed	100%	1/15/2003 7:14 AM	0:01:25	
Completed	DCS incremental		Backup	Canceled	N/A	1/15/2003 3:05 AM	4:01:13	0
Completed	Cleaning 0263		Cleaning	Canceled	N/A	1/15/2003 2:20 AM	0:02:55	0
Completed	TD Calendar Full	QUANTUM 4	Backup	Failed	Unknown	1/15/2003 2:09 AM	0:12:27	0
Completed	TDserver Incremental		Backup	Canceled	N/A	1/14/2003 11:55 PM	2:27:41	0
Completed	tdpc196	QUANTUM 4	Backup	Failed	Unknown	1/14/2003 2:24 PM	1:10:39	7,248,956,876
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/14/2003 3:05 AM	1:16:10	9,376,229,499
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/14/2003 2:09 AM	0:11:49	169,546,633
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/13/2003 11:55 PM	1:37:24	20,282,552,858
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/13/2003 3:05 AM	1:16:41	9,376,079,936
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/13/2003 2:09 AM	0:03:23	169,362,583
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/12/2003 3:26 AM	1:13:32	9,307,043,756
Completed	TDserver User Data	QUANTUM 5	Backup	Successful	100%	1/11/2003 11:13 AM	12:53:58	494,251,330,367
Completed	DCS	QUANTUM 4	Backup	Successful	100%	1/11/2003 4:02 AM	1:19:55	9,376,079,936
Completed	TDserver Op Sys	QUANTUM 5	Backup	Failed	Unknown	1/11/2003 3:59 AM	5:38:00	88,225,667,878
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/10/2003 11:55 PM	1:37:44	16,287,069,657
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/10/2003 10:29 AM	2:07:41	31,876,164,611
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/10/2003 3:05 AM	5:58:37	9,375,795,574
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/10/2003 2:09 AM	0:03:35	169,592,007
Completed	TDserver User Data	QUANTUM 5	Backup	Failed	Unknown	1/8/2003 9:43 PM	17:40:52	492,245,288,678
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/8/2003 3:05 AM	1:17:17	9,365,200,134

Backup Selections Restore Selections Job Definitions **Activity Monitor** Devices Media Reports Alerts

Ready TDARCHIVE

Start SGMon Backup Exec - [Activit...

11:50 AM



**Backup Exec - [Activity Monitor]**

File View Admin Network Select Jobs Tools Window Help

Backup Restore

## Scheduled, Active, and Completed Jobs

Class	Job Name	Device Name	Job Type	Job Status	Percent ...	Start Time	Elapsed Time	Byte Count
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/8/2003 2:09 AM	0:10:54	169,467,079
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/7/2003 11:55 PM	1:59:17	32,964,619,964
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/7/2003 5:06 PM	4:58:17	69,745,290,049
Completed	Erene's Reports	QUANTUM 4	Restore	Successful	100%	1/7/2003 10:00 AM	0:06:41	120,470
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/7/2003 3:05 AM	1:16:56	9,356,358,359
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/7/2003 2:09 AM	0:04:01	169,073,815
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	1/6/2003 11:55 PM	2:12:07	42,754,121,944
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/6/2003 3:05 AM	1:16:25	9,343,018,125
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/6/2003 2:09 AM	0:10:20	168,665,299
Completed	TDserver User Data	QUANTUM 5	Backup	Successful	100%	1/5/2003 12:08 PM	13:40:46	487,465,498,587
Completed	TDserver Op Sys	QUANTUM 5	Backup	Failed	Unknown	1/5/2003 3:19 AM	6:08:09	100,695,684,237
Completed	TD DBs	QUANTUM 4	Backup	Failed	Unknown	1/4/2003 1:04 PM	3:21:31	23,734,254,300
Completed	DCS	QUANTUM 4	Backup	Successful	100%	1/4/2003 4:02 AM	6:00:05	9,343,018,125
Completed	Cleaning 0253	QUANTUM 5	Cleaning	Successful	100%	1/3/2003 11:29 PM	13:19:31	0
Completed	Cleaning 0252	QUANTUM 4	Cleaning	Successful	100%	1/3/2003 11:28 PM	9:11:58	0
Completed	TDServer1 F	QUANTUM 5	Backup	Successful	100%	1/3/2003 10:36 PM	14:03:07	95,818,176,755
Completed	TDServer1 Project tdwebdb	QUANTUM 5	Backup	Successful	100%	1/3/2003 9:36 PM	7:39:52	66,002,142,750
Completed	Users CIS - ENG	QUANTUM 4	Backup	Successful	100%	1/3/2003 8:35 PM	11:56:02	163,721,713,181
Completed	Users HQ - SUP	QUANTUM 5	Backup	Successful	100%	1/3/2003 7:35 PM	5:51:37	69,956,147,297
Completed	TDPC206	QUANTUM 4	Backup	Successful	100%	1/3/2003 2:51 PM	6:33:17	1,518,917,544
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	1/3/2003 11:30 AM	5:28:49	9,343,018,125
Completed	tdsu03 home dirs (daily)	QUANTUM 5	Backup	Successful	100%	1/3/2003 11:30 AM	4:13:14	36,976,324,381
Completed	Restore 0250	QUANTUM 5	Restore	Successful	100%	1/3/2003 10:36 AM	0:04:48	6,800
Completed	Restore 0248	QUANTUM 5	Restore	Successful	100%	1/3/2003 10:24 AM	0:05:14	19,187,072
Completed	TDServer1 Project tdwebdb	QUANTUM 5	Backup	Successful	100%	1/1/2003 10:04 PM	4:44:36	65,949,957,791
Completed	Users HQ - SUP	QUANTUM 5	Backup	Successful	100%	1/1/2003 5:07 PM	5:31:38	70,177,567,173
Completed	Users CIS - ENG	QUANTUM 4	Backup	Successful	100%	1/1/2003 4:27 PM	11:28:37	163,544,784,871
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	1/1/2003 2:09 AM	0:02:53	168,337,179
Completed	TDserver User Data	QUANTUM 5	Backup	Failed	Unknown	1/1/2003 12:55 AM	10:13:20	188,981,272,192
Completed	tdsu03 home dirs (daily)	QUANTUM 5	Backup	Successful	100%	12/31/2002 8:30 PM	4:10:00	36,922,910,457

Backup Selections Restore Selections Job Definitions **Activity Monitor** Devices Media Reports Alerts

Ready TDARCHIVE

Start SGMon Backup Exec - [Activit... ClipBook Viewer 11:47 AM

**Backup Exec - [Activity Monitor]**

File View Admin Network Select Jobs Tools Window Help

Backup Restore

## Scheduled, Active, and Completed Jobs

Class	Job Name	Device Name	Job Type	Job Status	Percent ...	Start Time	Elapsed Time	Byte Count
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	12/31/2002 3:05 AM	1:18:54	9,343,018,067
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	12/31/2002 2:09 AM	0:02:26	168,337,179
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	12/30/2002 11:55 PM	1:21:14	17,690,909,309
Completed	tdsu03 home dirs (daily)	QUANTUM 5	Backup	Failed	Unknown	12/30/2002 8:30 PM	1:44:58	16,934,458,051
Completed	TDserver User Data	QUANTUM 5	Backup	Failed	Unknown	12/30/2002 3:48 PM	3:34:57	135,772,014,463
Completed	TDserver User Data	QUANTUM 4	Backup	Failed	Unknown	12/30/2002 1:54 PM	1:40:27	64,882,032,548
Completed	DCS	QUANTUM 4	Backup	Successful	100%	12/28/2002 4:02 AM	5:58:51	9,343,018,004
Completed	TDserver Op Sys	QUANTUM 5	Backup	Failed	Unknown	12/28/2002 3:00 AM	6:11:56	98,850,794,116
Completed	TDserver User Data	QUANTUM 4	Backup	Failed	Unknown	12/27/2002 11:43 PM	8:54:15	184,150,549,500
Completed	TDserver User Data	QUANTUM 5	Backup	Failed	Unknown	12/27/2002 7:28 PM	2:11:02	85,023,839,451
Completed	TDserver User Data	QUANTUM 4	Backup	Failed	Unknown	12/27/2002 12:21 PM	4:51:09	185,884,443,460
Completed	TDserver User Data	QUANTUM 4	Backup	Failed	Unknown	12/27/2002 11:53 AM	0:17:23	7,708,752,844
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	12/27/2002 2:09 AM	0:08:27	168,302,363
Completed	TDserver Op Sys	QUANTUM 5	Backup	Failed	Unknown	12/26/2002 2:15 AM	0:39:31	6,699,715,272
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	12/26/2002 2:09 AM	0:11:13	168,302,363
Completed	tdsu03 home dirs (daily)	QUANTUM 5	Backup	Successful	100%	12/25/2002 8:30 PM	4:09:16	36,890,180,272
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	12/25/2002 3:05 AM	1:18:32	9,343,018,004
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	12/25/2002 2:09 AM	0:09:30	168,302,363
Completed	tdsu03 home dirs (daily)	QUANTUM 5	Backup	Successful	100%	12/24/2002 8:30 PM	4:08:29	36,890,179,022
Completed	DCS incremental	QUANTUM 5	Backup	Successful	100%	12/24/2002 3:05 AM	1:18:05	9,343,018,004
Completed	TD Calendar Full	QUANTUM 4	Backup	Failed	Unknown	12/24/2002 2:09 AM	0:09:48	166,509,847
Completed	tdsu03 home dirs (daily)	QUANTUM 5	Backup	Successful	100%	12/23/2002 8:30 PM	4:08:57	36,890,177,772
Completed	DCS incremental	QUANTUM 5	Backup	Failed	Unknown	12/23/2002 3:05 AM	0:26:52	2,249,885,533
Completed	TD Calendar Full	QUANTUM 4	Backup	Successful	100%	12/23/2002 2:09 AM	0:11:49	168,266,523
Completed	DCS	QUANTUM 4	Backup	Successful	100%	12/21/2002 4:02 AM	9:55:39	9,339,894,917
Completed	TDserver User Data	QUANTUM 4	Backup	Failed	Unknown	12/21/2002 12:27 AM	12:12:31	185,646,135,135
Completed	Catalogs 12/20	QUANTUM 4	Backup	Successful	100%	12/20/2002 11:45 PM	0:29:35	6,741,328,600
Completed	tdsu03 home dirs (daily)	QUANTUM 5	Backup	Successful	100%	12/20/2002 5:57 PM	4:08:28	36,873,911,606
Completed	TDserver Incremental	QUANTUM 5	Backup	Failed	Unknown	12/20/2002 3:19 PM	0:53:51	9,679,895,945
Completed	tdport30 2	QUANTUM 4	Backup	Failed	Unknown	12/20/2002 2:34 PM	0:07:01	41,252,097

Backup Selections Restore Selections Job Definitions **Activity Monitor** Devices Media Reports Alerts

Ready TDARCHIVE

Start SGMon Backup Exec - [Activit...

11:25 AM

# Fermilab Policy on Computing

## **Abstract**

*This is an abstract of the Fermilab Policy on Computing. The full text of the Policy follows the abstract at <http://www.fnal.gov/cd/main/cpolicy.html>. For details and who to go to when authorization for an activity is required, please consult the full text of the Policy. If you find something unclear or ambiguous in this abstract, see the full Policy for the final word. Feel free to address questions to Irwin Gaines (x4022, [gaines@fnal.gov](mailto:gaines@fnal.gov)) or to another computer security person listed in the Policy's section on "Roles".*

Fermilab's Policy on Computing covers all Fermilab-owned systems and all systems, regardless of ownership, when connected to our network (or showing a Fermilab address). You are responsible for the actions of any person whom you permit to use Fermilab computing or network resources through an account assigned to you.

## **Appropriate Use**

Fermilab encourages effective use of computing technologies in all aspects of its activities. Fermilab maintains an open scientific environment where the free exchange of ideas is encouraged and protected. We permit a wide range of computer activities including incidental use for private purposes. We encourage use of the Web and other Internet communication channels. With this comes the responsibility for every Fermilab employee and user to exercise common sense and good judgment.

Our policy is consistent with Federal (GSA) guidelines. However, many members of the public do not understand the scientific culture of openness and may question a posting (or email) that shows an FNAL.GOV address if it is not clearly related to Fermilab's scientific mission. Therefore, from a Fermilab address you should avoid highly visible activities on newsgroups, auctions, game sites, etc., that are not clearly Fermilab business. In particular, avoid all such Internet activities that are in competitive and/or contentious environments (auctions, political news groups, etc.) and avoid acting as a public server of music or other media unrelated to our mission. It is Fermilab policy to respect the intellectual property rights of others including copyrights, trademarks, and software licenses.

Use common sense in displaying links on pages with Fermilab addresses. Web crawlers (Yahoo, etc.) index all pages they can see. Even accidentally inappropriate wording may be indexed. You can direct web crawlers to ignore pages that you do not need to be found through search engines. See <http://www.fnal.gov/cd/webgroup/webhelp/access.html>. Semi-official pages and pages intended for the public are required by the DOE to carry a notice. Include a link on each such page to <http://www.fnal.gov/pub/disclaim.html>

The following are explicitly NOT permitted:

- ☐ Legally prohibited activities;
- ☐ Activities that reasonably offend other employees, users, or outsiders, or results in public embarrassment to the laboratory;

- ☐ Activities in support of an ongoing private business;
- ☐ Up- or down- loading or viewing of sexually explicit material.

You must have specific approval for activities that consume significant amounts of computer or network resources whether for lab or personal purposes.

### ***Rules to Protect Fermilab Computing***

Our first lines of defense are the individuals responsible for data and the local system managers. Proper use and protection of passwords, physical protection of computers, and regular backup of important data are required. The Fermilab Policy on Computing includes a minimal set of strongly enforced specific rules. In addition, any form of blatant disregard for computer security is not tolerated.

- ☐ You are required to immediately report any suspected computer security incidents to 630-840-2345. The Fermilab Computer Incident Response Team (FCIRT) investigates incidents. The Head of FCIRT may assume full administrative control of affected systems until the incident is resolved, call on other experts for priority assistance and direct local system managers to respond to the situation. You may not disclose information regarding a computer security incident without authorization.
- ☐ Hacking is forbidden, including unauthorized attempts to gain access, to damage, alter, falsify, or delete data, to falsify email or network address information, or to cause a denial of computing or network service. The use or possession of security-probing or cracker tools requires written authorization.
- ☐ You may not implement network or email infrastructure services without written authorization.
- ☐ If you have privileged access to three or more systems, to a major clustered system, or to any computer within a critical system domain, you are required to register through the web form at <http://miscomp.fnal.gov/sysadmindb> and to follow security guidelines.
- ☐ No one may inspect another person's files or email without that person's permission or other authorization, explicit or implicit, as described in the Policy.
- ☐ You must not allow anyone else to know or use your Kerberos password. Don't use your Kerberos password for other than Fermilab Kerberos. Do not transmit Kerberos passwords (or the character string of a Kerberos password) across the network. In the rare circumstances where transmitting a Kerberos password is necessary, it must be strongly encrypted. Never store Kerberos passwords (or the corresponding character strings) on a computer, encrypted or not. Configuration rules for Kerberos-protected systems must not be circumvented.
- ☐ In urgent situations, the Fermilab Computer Security Coordinator (FCSC) may declare certain configurations to be a Critical Vulnerability. This designation and corrective action will be publicized as widely as possible. You are required to take immediate action to remove Critical Vulnerabilities from systems under your control.

### ***Use of Computers in Systems that Protect People, Property, or the Environment***

Fermilab policy is to avoid reliance on a computer as an essential element of any system that is necessary to protect people from serious harm, to protect the environment from significant impact, or to protect property the loss of which would have a serious impact on our mission. The use of computers for monitoring, data logging, and reporting is encouraged, however computers used for these purposes must not be essential for protection. Contact the Fermilab Computer Security Executive for any variance.

## ***Fermilab Policy on Computing***

Advances in the basic understanding of elementary particles have through a long history been enabled by the ever-changing frontiers of technology. Computing has always been one of the key technologies that enable the science, and this is particularly true today. Fermilab encourages effective progressive use of computing technologies in all aspects of its activities, recognizing that this brings with it special, always evolving, concerns.

Computing is one of many tools used at Fermilab and, as such, general policies, written and unwritten, that govern life at Fermilab apply equally to computing. For example, it is obvious that the same rules of ethical behavior apply regarding fraud, forgery, plagiarism, harassment, libel, etc. whether computers are involved or not. However, the ability of modern computers and networks to manipulate, store, and broadcast information is so extraordinarily powerful that it changes many qualitative aspects of how we function in a research laboratory, often in dramatic ways.

The policies and rules described in the following are intended to address these special aspects of computing at Fermilab. The policy is divided into four sections:

- ☐ Policies and Rules to Protect Fermilab Computing
- ☐ Publishing and Accessing Information on Electronic Networks
- ☐ Use of Computers in Systems that Protect People, Property, or the Environment

### **1. Policies and Rules to Protect Fermilab Computing**

The communications needs for research and planning require a broad openness in our systems. Our main concerns are protecting data and systems critical to the operations of the laboratory in pursuit of its mission. Fermilab's continuing policy has been to put its first line of defense at the individual responsible for the data and the local system manager. Proper use of passwords and, most importantly, backup of important data is what we expect of our computer users and system managers.

#### **Roles**

The Director has delegated overall responsibility for computer security and related matters to the Fermilab Senior Computer Security Executive (CSExec). The Fermilab Computer Security Coordinator (FCSC)<sup>1</sup> FCSC reports to the CSExec in this area, and is

---

<sup>1</sup> The CSExec responsibility is currently assigned to the Computing Division Head, Victoria White, 630 840 3936, white@fnal.gov. Dane Skow, 630 840 4730, dane@fnal.gov, is Deputy CSExec. The FCSC role has much in common with what was previously called the Computer Protection Program Manager (CPPM). The FCSC is Matt Crawford, 630 840 3461, crawdad@fnal.gov. The General Security Domain Coordinator is Irwin Gaines, 630 840 4022, gaines@fnal.gov. Donna Dyxin is the Deputy FCSC for Government Liaison, 630 840 8849, ddyxin@fnal.gov. The Head of the Fermilab Computer Incident Response Team (FCIRT) is Mark Kaletka, 630 840 2965, kaletka@fnal.gov.

the laboratory's principal day to day computer security manager and lead point of contact with external organizations (DOE, FBI, CIAC, etc.) on computer security. In the latter role, the Deputy FCSC for Government Liaison assists the FCSC, particularly in handling policy communications with the DOE. A second Deputy FCSC is the General Security Domain Coordinator.

## **Scope**

Fermilab's Computer Security Policy covers Fermilab systems<sup>2</sup>, whether on-site and connected directly to the Fermilab network, or on- or off-site and connected to the Fermilab network by the telephone system, the Internet, or other means. The policy and rules described here cover these systems no matter who is the owner or the method of connection to the network.

Not included are those activities by users of off-site computers that do not involve, and do not give the appearance of involving<sup>3</sup>, computers on the Fermilab site network.

Additional security rules apply to the configuration of all on-site or off-site computers within Fermilab's "Strengthened Realm".<sup>4</sup>

Fermilab employees and registered users are responsible for their own actions under the computer security policy, as well as for the actions of any person who they permit to access a Fermilab system.<sup>5</sup>

## **Appropriate Use**

Fermilab's single mission is science and the laboratory's stated policy is to maintain an open scientific environment where the free exchange of ideas is encouraged and protected. We want there to be unhindered freedom to use computers within a wide area, but this area is surrounded by extremely high walls. We cannot always describe exactly where those boundaries lie, because the technology is changing rapidly and because the walls may shift with shifts in the public's tolerance and areas of scrutiny. Those who use Fermilab's computers and networks will have to use judgment and common sense when

---

<sup>2</sup> "Fermilab systems" are those which are connected to the network and show an address or name within a Fermilab network or domain (e.g. 131.225.\*.\*,fnal.gov, sdss.org, auger.org, etc.), as well as systems not connected to the network but owned by Fermilab.

<sup>3</sup> Show an address, name, or email address within a Fermilab network or domain (e.g. 131.225.\*.\*,fnal.gov, sdss.org, auger.org, etc.).

<sup>4</sup> On-site or off-site computers in the "Strengthened Realm" are those on which users may be authenticated for access to systems on the Fermilab network by a Fermilab Kerberos Key Server.

<sup>5</sup> Some operating system user identifiers (such as root or Administrator) are understood to be commonly shared by several people. Other user identifiers are explicitly shared for various roles or projects. A user's Kerberos identifier is never to be shared. The proper way to share access to a Kerberos-protected resource or service is to list the user principals in an ACL file such as .k5login.

they operate near the edges of acceptable use. Examples of activity that may bring an employee or user near or past walls of acceptable usage and incur serious disciplinary repercussions (or, in certain cases, criminal sanctions) are:

- ☐ Legally prohibited activities on the Internet (child pornography, interstate gambling,...);
- ☐ Computer usage that reasonably offends other employees, users, or outsiders, or results in public embarrassment to the laboratory;
- ☐ Computer usage that is not specifically approved and which consumes significant amounts of computer resources not commensurate with its benefit to the laboratory's mission or which interferes with the performance of an employee's assigned job responsibilities;
- ☐ Operation of a private business or social activity unrelated to the laboratory;
- ☐ Violation of license and other computer related contract provisions, particularly those that expose the laboratory to significant legal costs or damages.

Questions of proper or improper use of computers are normally management rather than technical issues and should be dealt with in the normal course of supervisory oversight. Fermilab policy requires rapid response investigation of incidents involving extreme behavior, as well as preventive monitoring where there is reasonable cause.

## **Rules**

Fermilab has a minimal set of rules that will be enforced. They address incident reporting, protection of system and network integrity, prohibitions against unauthorized activities, ethical behavior, etc. They address matters serious enough that the laboratory is willing to enforce disciplinary measures for first offenses, such as suspending employees or barring users from laboratory facilities.

### *Incident Reporting*

All employees and users are required to immediately report any suspicious incidents involving the security of Fermilab computers or networks, including apparent attempts at unauthorized access. Incidents should be reported to the Feynman Computing Center 24x7 Customer Support Help Desk at +1 630-840-2345, or to the system manager if immediately available. System managers are expected to report incidents immediately that do not have a simple explanation based on normal routine operation of the system. If there is clearly no urgency, incidents may be reported by email to [computer\\_security@fnal.gov](mailto:computer_security@fnal.gov).

Incidents which must be reported include computer- or network-related activity, internal or external to Fermilab, that may impact Fermilab's mission through, for example, the possibility of: loss of data; denial of services; compromise of computer security; unauthorized access to data that Fermilab is required to control by law, regulation, or DOE orders; investigative activity by legal, law



enforcement, bureaucratic, or political authorities, or a public relations embarrassment.

The Fermilab Computer Incident Response Team (FCIRT), appointed by the CSExec, will investigate all reported incidents. Incidents are quickly triaged by FCIRT. During particularly serious incidents known as “FIRES”<sup>6</sup> the Head of FCIRT may assume full administrative control of affected systems until the incident is resolved, and may call on other technical experts for priority assistance. For incidents with localized implications, the Head of FCIRT may declare a “SMOKE”<sup>7</sup> and direct local system managers to respond to the situation under the oversight of FCIRT.

Employees and users must not disclose information resulting from a computer security incident without authorization. The head of the FCIRT and the CSExec, in consultation with the head of the Computing Division and the Public Information Office, will determine specific information to be disclosed to employees, users, other organizations, and the public.

### *Unauthorized and Malicious Access and Actions*

All employees and users are forbidden to attempt unauthorized entry to computer systems or accounts, or to attempt unauthorized damage, alteration, falsification or deletion of data (including software and email). This prohibition explicitly includes attempts to spoof or falsify email, network, or other information used to identify sources, destinations or other information about communications, data, or storage. Individuals are implicitly authorized to access accounts in their own name, and to alter or delete data in those accounts, and they may access files which are enabled for reading for a class of individuals including the person attempting to access them. The burden of proof of authorization rests with the person attempting to access an account; possession of a password is not proof of authorization. All employees and users are forbidden to attempt to cause denial of computing or network services at Fermilab. Serious negligence that results in service denials will be treated as any other negligence that results in equivalent damage to the laboratory mission.

### *Blatant Disregard for Laboratory Computer Security*

Blatant disregard for Laboratory computer security will not be tolerated. The FCSC or Head of FCIRT (or their designees) may advise individual employees or users that specific computer security practices are unacceptable in a way which unreasonably exposes Fermilab computers or increases the effort required by computer security personnel, and that they should correct these unreasonable practices. Email records of such “warnings” or “advisories” will be maintained by the FCSC’s organization. If an employee who has received such a written “warning” or “advisory” about an unacceptable practice is found, either through routine security evaluations or through an FCIRT investigation of an incident, to

---

<sup>6</sup> “Fermilab Incident Response Emergency”

<sup>77</sup> “System Manager’s OKurrence Evaluation”

be again in violation in regard to this practice, the FCSC will refer the case to the CSExec for disciplinary action.

Individuals who, by reason of their actions or the configuration or content of computer systems for which they are responsible, have been implicated as a significant factor causing a serious computer security incident (FCIRT triaged as a SMOKE or FIRE) should become especially aware of computer security rules and guidance. Being implicated as a significant factor in a subsequent serious computer security incident will be taken as *prima facie* evidence of blatant disregard for computer security.

### *Restricted Central Services*

The following services may only be implemented by Computing Division personnel authorized in writing by the Computing Division Data Communications Group Leader, or as otherwise noted:

Routing and bridging, except that the Beams Division runs its own subnets.

Tunneling, except tunnels with a single source or destination for purposes of mobility or security.

All forms of off-site network connection except modems.

DHCP.

Assignment of IP and DECNET host names and addresses. (Use of automatic configuration mechanisms provided by the Computing Division Data Communications Group, such as DHCP, are not restricted.)

DNS zone mastering and all externally-reachable DNS service.

NTP time service at stratum 1. (Stratum 2 server operation is discouraged.)

NNTP.

Specific waivers from these restrictions must be in writing and may be granted only by the FCSC or the Computing Division Data Communications Group Leader. Waivers granted to non Fermilab employees require the concurrence of the CSExec.

The following services are also restricted. Exceptional approval for professionally managed workgroup-local implementation will be considered by the FCSC.

- ☐ Externally-reachable email servers, including SMTP, POP and IMAP.
- ☐ Externally-reachable web servers
- ☐ Kerberos key servers.

## *Security and Cracker (or Hacker) Tools*

A “security tool” is a tool with the capability to systematically probe, or otherwise gather information about, a system or network in order to discover security vulnerabilities. A “cracker tool” (often referred to as a “hacker tool”) is a tool with the capability to systematically exploit security vulnerabilities in order to attempt unauthorized access, destruction or theft of data, denial of service, or other unauthorized activities. The use of any tool as a security or cracker tools, or the possession of any tool whose principal capability is as a security or cracker tool or to disguise or facilitate cracking or security probing activities, by employees and users is limited to the specific tools, time frame, and purpose, in explicit written authorization signed by the CSExec or FCSC.

## *System Managers*

Employees and users who have root/system/administrator password access to three or more systems, or to a major clustered system, or to a computer within a critical system domain, are required to register with the FCSC (via the web form at <http://miscomp.fnal.gov/sysadmindb>) so they may be reached to provide assistance during a computer security incident response. They will be asked to maintain a list of all systems for which they have root access. All system managers will be expected to follow sound system security guidelines as developed by the Computing Division.

System managers may access all “system” accounts and files on systems for which they have responsibility. “System” accounts and files are those not specifically assigned to an individual. In the course of normal system maintenance activities they may disable the computer or its network connections and they may work with an individual's account or files with the following restrictions: they may not physically (in the human sense) read or inspect the data or information in them (except for files enabled for reading by a class of individuals including the person attempting to read them), and they may not change or delete files in a way that precludes recovering the original data. A person has “system manager responsibility”, if a) he/she is registered in the System Manager Data Base for that system; or b) the system is assigned as an individual computer or workstation to the person (and registered in the sensitive item database if applicable).

## *Data Integrity and Backup*

Users (“data owners”) are responsible for determining what data requires protection and how their data is to be recovered if the online copy is destroyed (either by accidental or malicious damage). They may choose not to back up data, but if so they must make sure they know how to recreate the lost data if needed. If backup is necessary then the users must coordinate a backup plan. This may either be an individual backup done by the users themselves or coordinated with the system managers into a regular system backup plan.

System managers are responsible for carrying out the backup plans for the systems they manage. They are expected to publish to their users the following: a) which files and data on the system are backed up and which are not; b) backup procedures including frequency of backup, type of backup (full or incremental), media, procedure for restoring files, and location of media storage; c) any special local storage management policies (e.g. automatic purging of backed up areas). System managers are also responsible for periodically testing restoration procedures and for recording the dates of backups, success or failure, and results of restoration tests.

### *Protection of Kerberos Passwords*

You must not allow anyone else to know or use your Kerberos password. Don't use your Kerberos password for other than Fermilab Kerberos. Do not transmit Kerberos passwords (or the character string of a Kerberos password) across the network. In the rare circumstances where transmitting a Kerberos password is necessary, it must be strongly encrypted. Never store Kerberos passwords (or the corresponding character strings) on a computer, encrypted or not. Configuration rules for Kerberos-protected systems must not be circumvented.

### *Critical Vulnerabilities*

In urgent situations, the Fermilab Computer Security Coordinator (FCSC) may declare certain configurations to be a Critical Vulnerability. This designation and corrective action will be publicized as widely as possible. You are required to take immediate action to remove Critical Vulnerabilities from systems under your control.

## **Division/Section/Large Experiment Rules**

Divisions and sections and large experiments<sup>8</sup> may establish security rules or guidelines for systems under their management. These may be enforced by disabling access for a user who is in violation.

## **Critical Systems**

Computer security incidents involving certain systems could seriously impact the laboratory's science programmatic operations. Such systems may be designated "critical systems" and may be subject to additional computer security policies and procedures, beyond those described here.

---

<sup>8</sup> At this time, "large experiments" include CDF and D0. In the future, other active major experiments, such as CMS, MINOS, etc., will be added to this list.

## Access Control

*[Most of this subsection is technical and addressed at system managers.]*

The motivation for Fermilab's move to a strong authentication realm includes the following goals:

- ☐ elimination of clear text passwords on the network,
- ☐ elimination of crackable password files on systems,
- ☐ a single password and/or cryptocard for each user,
- ☐ the expectation of the United States Government that Fermilab management will exercise positive control of those who use the government's resources, including Department of Energy owned computers and the network, at the Fermilab site,
- ☐ maintaining the free and open access to Fermilab's scientific activities and information by the international high energy physics community.

Consistent with the motivations cited above, we do not require Kerberos authentication for uses which involve only reading information (via the Web or ftp, for example), or only entering information into a Web or data base form<sup>9</sup>, even if a password is required by the local organization or collaboration. All other uses of computers or the network within a strengthened realm must be preceded by Kerberos authentication that will verify that the user is either a Fermilab employee or an onsite or offsite user who has registered with the Users' Office. This does not mean that all computers or applications within the strengthened realm are required to use Kerberos authentication. It does mean that before using a computer that does not do Kerberos authentication an individual must pass through either a computer that does a Kerberos authentication or through a computer to which physical access is restricted to individuals carrying a valid Fermilab ID card .

The following policies are in force for protection of user authentication. Distinctions are made between systems on-site and those at visitors' home institutions. For all on-site systems, all network access which provides access comparable to system login, shell execution or file transfers (other than anonymous) must only be authenticated by Kerberos credentials presented with the connection setup, or by a single-use authentication mechanism (such as a Cryptocard) tied to the Kerberos infrastructure. Off-site systems may optionally accept encrypted connections using non-Kerberos authentication mechanisms, but such connections may not be used for sessions that connect to Fermilab.

---

<sup>9</sup> It is required that a user be Kerberos authenticated within the Strengthened Realm prior to that user entering information into a form on a computer in the Strengthened Realm for any purpose where incorrect or inappropriate entry could cause damage to Fermilab resources or disruption to Fermilab activities. This includes, but is not limited to, entry of data to be used to set control values for equipment (including accelerator, beam, detector, building, etc.) or to be used for computer system management or configuration purposes.

In any case, offsite systems joining a Fermilab Kerberos realm must be covered by a written policy stating that insecure access mechanisms (including cleartext reusable passwords and "traditional r-command" methods) will not be permitted, and must adhere to said policy.<sup>10</sup>

On- and off-site systems in our Kerberos realm will be probed over the network to try to verify compliance with these conditions. Hosts found to be noncompliant may be barred from obtaining Kerberos tickets from our realm. If the noncompliance is deliberate or extremely careless it may be deemed to constitute blatant disregard for computer security.

### **Privacy of Electronic Files and Email**

In normal day to day activities, Fermilab respects the privacy of the electronic files and email of employees and visitors, and it expects all employees and visitors to do likewise. No one may inspect the files or email belonging to anyone else on a Fermilab computer without that person's permission, either explicit or implicit as described above in the rule "Unauthorized and Malicious Access and Actions". [What system managers may do without further authorization is described above in the rule "System Managers".]

No person may use, for any purpose whatsoever, any information in another person's files (including e-mail) that they have seen incidental to any legitimate or illegitimate activity without either a reasonable belief that the file was meant to be accessed by others or the explicit permission of the person to which the file is assigned. It may be implicitly presumed that files shared by an experimental collaboration or other workgroup have the permission of all members of the group to be used by other members for purposes related to the mission of the group. An employee's (or user's) files, with the exception of files on backup media, that remain after the employee termination process is completed (expiration of user's validation) may be transferred as directed by the employee's supervisor (user's spokesperson) without further permission.

The following paragraph describes a standing exemption from these restrictions for specified computer security personal. Other exceptions to these restrictions require the written approval of the Director, Deputy Director, or an Associate Director (with copies of these approvals maintained in the Office of the CSExec). Such exceptions will normally be made only in serious disciplinary or legal situations.

Members of the Fermilab Computer Incident Response Team (FCIRT) as well as the FCSC and Deputy FCSCs may monitor computing activities and access and inspect any files or email in the course of carrying out their computer security preventive and response functions. Information learned in this way which is pertinent to computer security may be shared discreetly with others including supervisors and local system managers. Information not pertinent to computer security will be kept in confidence.

---

<sup>10</sup> It is expected that the written policy will list the systems covered by this policy and what combinations of access (e.g., ssh, telnet, ipsec) and authentication (RSA keys, passwords, one-time passwords, etc.) are allowed on those systems. It must also give a means of contacting the system administrator(s). If a written policy against allowing insecure access to such systems meeting these requirements already exists, it may be used. If nothing exists, one can be drawn up for the purpose.

Evidence of egregious behavior (serious violations of Fermilab rules, criminal activity, etc.) that is uncovered incidental to such computer security related inspections will be reported to the CSExec for possible action through the Laboratory's normal channels.

### **Software Intellectual Property (Licenses)**

Employees and users of Fermilab computing are reminded that it is Fermilab policy to respect the intellectual property rights of others. This applies when computers are involved just as it does when computers are not involved. Fermilab expects reasonable care be taken to follow license provisions.

## **2. Publishing and Accessing Information on Electronic Networks**

The technology of the international computer network (Internet) and the evolving applications and standards that support it (especially the World Wide Web) provide unprecedented power to access and publish information almost instantaneously. Its impact on the collaborative field of high energy physics is particularly profound. It is an ideal tool for communication in the field. Fermilab strongly encourages its use.

This new capability comes with new challenges and individual responsibilities since this technology invites a much more immediate and wide dissemination of information. Despite the new power of this technology, the fundamental policy of Fermilab, and of its parent agency, about information and the use of our computers and networks remains unchanging and simple:

- ☐ Fermilab's single mission is science and the laboratory will maintain an open scientific environment where the free exchange of ideas is encouraged and protected.
- ☐ The use of government property is for the government's purposes.

There is no real conflict between these two principles since Fermilab's mission is for the government's purposes. The problem is in the interpretation of which ideas and what information are in the interests of Fermilab's science and open environment. Fermilab's policy is to take the broadest possible interpretation. There is a large gray area, and, to protect the continuing free exchange of ideas, it is the responsibility of every Fermilab employee and user to use common sense and good judgment.

Some material is not in the gray area. Sexually related material is clearly inappropriate, and when found either on Fermilab computers or posted externally from a Fermilab network address, Fermilab will initiate disciplinary action, including suspension without pay for employees, or suspension of site and computer access privileges, for users. In some cases, certainly those involving the felonious possession of pornography involving children, the government will take criminal action. Other legally prohibited material could also bring severe disciplinary or criminal sanctions.

Many people access the network and its postings. Most of them are from outside the scientific culture, and they may not understand how a particular posting may be related to the government's business. Therefore, it is Fermilab's policy that material that is published or posted with external visibility must be predominately clearly related to Fermilab's scientific mission.

The ease of use of this technology breaks down traditional mechanical barriers to publication prior to review. The disappearance of these barriers does not permit bypassing established rules and procedures regarding publication. For the purposes of these rules and procedures, electronically posted information with visibility external to the Fermilab community is to be understood as a public document.



The many crosslinks possible (on The Web, for example), and their ephemeral nature, means that pointers (links) to external addresses can quickly become a source of embarrassment. Employees and users should use common sense in displaying links on pages with Fermilab addresses; a link should only point to material that is predominately appropriate reference material -- and likely to stay that way.

## **Scope**

The policies described in this document apply to material posted on or retrieved from network addresses or domains owned or managed by Fermilab (e.g., fnal.gov, fnal.org, hep.net, auger.org, sdss.org, vlhc.org, scitech.mus.il.us, etc.). The applicability is not determined by who owns the computer or whether the data is physically stored on site or offsite or by the method of connection to the network. Fermilab employees and registered users are responsible for their own actions under this policy, as well as for the actions of any person who they permit to access a Fermilab computer system to post or retrieve material.

## **Public Availability versus Restricted Access**

As an institution whose primary mission is to produce and disseminate new scientific information, Fermilab encourages the unrestricted publication on the Internet of as much of its internal material as possible. However, there may be reasons to restrict access to specific material, for example, its proprietary nature, security considerations, possibility of misinterpretations that could cause embarrassment, scientific work in progress, etc.

Division/Section Heads and Spokespersons are responsible for determining the classes of material within their organizations that should be restricted for access only by the Fermilab community or by defined subsets of the Fermilab community. The Computing Division World Wide Web Group will provide detailed instructions on implementing various options to restrict access for popular web servers. Options include restriction by password or IP address.

## **Material Intended for the Lay or Scientific Public**

The Head of the Directorate's Office of Public Affairs has the responsibility for maintaining a home page and auxiliary pages presenting Fermilab to the public. Other laboratory entities may also provide such public information. In each such case where material is intended for the broad lay or scientific public, there must be an individual, approved in writing by the Head of Public Affairs, a Division/Section Head, or a Scientific Spokesperson, and identified on the electronic page, with responsibility for the material.

## **Externally Accessible Material Not Intended for the Lay or Scientific Public**

Approvals are not required for material that is externally accessible but not intended primarily for the public. However, such material is subject to this policy and

Division/Section or Spokesperson policy on content that may be posted for external access.

### **Professional (Personal) Home Pages**

Individuals may publish professional (personal) home pages subject to this policy and to the policy of their Division/Section Head or Spokesperson as to content which may be posted for external access.

### **Semi-Official and Public Web Pages**

Semi-official and pages intended for the public web pages require special considerations. The following would be examples of pages with unrestricted external access that are considered to be "semi-official":

- ☐ the page indicates that it is sponsored by a division, section, department, experiment, or other laboratory sanctioned organization
- ☐ it provides general institutional and/or technical information to laboratory staff, visitors, or the public
- ☐ it makes available a general laboratory service that is part of the mission of a Division, Section, or Department.

We do not include in this category pages that are working documents, such as computer codes, technical papers, professional home pages, etc.

The public and government agencies subject to particular scrutiny semi-official pages and pages intended for the public that have a .gov address. Division, section, and experiment management should pay particular attention that the content of these pages be generally seen as appropriate and inoffensive.

Semi-official pages and pages intended for the public are required by the Department of Energy to carry a legal notice. This notice should be implemented by including a link on each such page to <http://www.fnal.gov/pub/disclaim.html>

### **Web Crawler Controls**

Web crawlers such as Google, Yahoo or FirstGov, may index all pages with unrestricted external access. Even accidentally inappropriate wording (in computer codes or minutes, for example) are likely to be indexed and provide fodder for the salacious-minded.

Relatively simple methods exist for directing cooperating web crawlers, or "robots", not to index certain web sites or follow links found there. Consult the guidance document at <http://computing.fnal.gov/cd/web/publish/access.html>.

A preference not to index should only be used on working documents. Because the public or off site members of the Fermilab community may have a need to search in a public web crawler for information in Semi-Official pages, such pages should not be marked

“do not index”.

### **Cookies**

The DOE strongly discourages the use of cookies. They should not be used on web pages intended for the general public. If you have a very strong technical or administrative reason to use cookies on a page intended for internal use, check with the computer security organization for guidance. There are no restrictions on the use of cookies on pages that are not visible from off-site.

### **Collecting Information from Children**

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. It is Fermilab policy not to collect personal information from children under 13.

### **Privacy and Information Collected from the Public**

It is Fermilab policy that any information collected electronically from the public not be used for any external or commercial purposes, whether this information was collected intentionally or not. You should deal with any such collected information in conformance with the Fermilab Privacy Notice published at <http://www.fnal.gov/pub/disclaim.html>.

### **3. Use of Computers in Systems that Protect People, Property, or the Environment**

Since the earliest days at Fermilab, it has been our policy to avoid reliance on a computer as an essential element of any system that is necessary to protect people from serious harm, to protect the environment from significant impact, or to protect property the loss of which would have a serious impact on our mission.

The use of computers for monitoring, data logging, and reporting is encouraged, however computers used for these purposes must not be essential for protection.

Any variation from this policy on protection systems must have the written concurrence of the Fermilab Senior Computer Security Executive (CSExec) and the Associate Director for Operations Support (ADOS).

A committee appointed by the CSExec and ADOS will consider variances from this policy for systems designed in accord with ANSI/ISA S84.01-1996 at level 3 (or under IEC 61508 standard, levels 3 or 4) after a detailed review of the plan. In particular, the system must be isolated from the Laboratory network and the Internet at all times, and its program must never have been exposed to these networks and must be traceable to program source code that has been reviewed by the above committee.

Publication Date: August 20, 1998

Revision: June 4, 2002

Revision: April 9, 2004

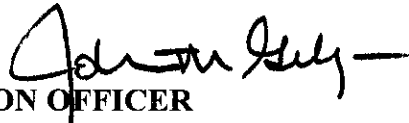


## Department of Energy

Washington, DC 20585

July 26, 1999

**MEMORANDUM FOR: LEAD PROGRAM SECRETARIAL OFFICES**

**FROM: JOHN M. GILLIGAN**   
**CHIEF INFORMATION OFFICER**

**SUBJECT: UNCLASSIFIED COMPUTER SECURITY PROGRAM**

**DOE N 205.1 UNCLASSIFIED COMPUTER SECURITY PROGRAM** has been issued. This notice cancels **DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM**, dated 5-18-92. This notice is effective immediately.

The policy is issued as a notice and additional policy and guidance will be required in the area of unclassified computing. This will be worked in a rapid fashion and will be issued upon completion.

Please forward any comments to Pete Salatti, of my staff, 301-903-4477, E-mail [pete.salatti@hq.doe.gov](mailto:pete.salatti@hq.doe.gov).

cc: All Departmental Elements





## Department of Energy

Washington, DC 20585

9 8 1999 .1111 2 6 1999

MEMORANDUM FOR: JOHN M. GILLIGAN  
CHIEF INFORMATION OFFICER

FROM: *John Wilczynski*  
JOHN WILCYNISKI, DIRECTOR  
OFFICE OF FIELD INTEGRATION

SUBJECT: Field Management Council Review Request,  
9906-MA011.000

REFERENCE: Memorandum Entitled, "Department of Energy Notice  
DOE N 205.1, Unclassified Cyber Security Policy"

The Lead Program Secretarial Offices (LPSO) have reviewed your request through the Field Management Council (FMC) process and the Deputy Secretary has approved the issuance of the subject memorandum as revised.

Your office is now authorized to issue the memorandum to the field elements with copies to the LPSOs and Field Integration (FI). All information provided to the field, the LPSOs, and FI should be transmitted electronically.

If you have any questions or comment concerning this action, contact the Office of Field Integration, Skip Castro, at extension 6-4937.

### Attachment

cc: DP-1  
EM-1  
SC-1  
EE-1  
FE-1  
NE-1  
RW-1  
MD-1  
NN-1



**U.S. Department of Energy**  
**Washington, D.C.**

**NOTICE**

DOE N 205.1

Approved: 7-26-99

**SUBJECT: UNCLASSIFIED CYBER SECURITY PROGRAM**

---

1. OBJECTIVES.

- a. To establish the framework for the Department of Energy (DOE) Unclassified Cyber Security Program.
- b. To set forth requirements and responsibilities for protecting all unclassified DOE information and information systems in order to maintain national security and ensure that DOE business operations proceed effectively.
- c. To ensure that the DOE Unclassified Cyber Security Program achieves the objectives of Federal and State regulations, Executive Orders, national security directives, and other regulations.
- d. To establish best business practices (i.e., requirements) for protecting DOE information and information systems, which include provisions for ensuring that the protection of information systems is commensurate with the risk and magnitude of harm that could result from the loss, misuse, disclosure, or unauthorized modification of information processed, stored, or transmitted using the Department's information systems.
- e. To ensure that the confidentiality, integrity, availability, and accountability of information is preserved by any information system that is used to acquire, store, manipulate, manage, move, control, display, switch, interchange, receive, or transmit that information.
- f. To establish an agile approach to DOE information processing systems security to keep pace with rapidly changing threats, vulnerabilities, missions, and technologies.
- g. To require that Department-wide guidance on the Unclassified Cyber Security Program is updated on a continuing basis.

---

**DISTRIBUTION:**

All Department Elements

**INITIATED BY:**

Office of the Chief Information Officer

- h. To require that each DOE Headquarters and field element, to include DOE Federal organizations and DOE contractor organizations, tailors the protection mechanisms, implementation, and security planning for its Unclassified Cyber Security Program to suit its environment, missions, and threats, while maintaining consistency and interoperability within applicable mission interoperability clusters.
    - i. To implement the requirements of Office of Management and Budget, Circular A-130, Appendix III.
- 2. CANCELLATION. This Notice cancels DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, dated 5-18-92.
- 3. APPLICABILITY.
  - a. This Notice applies to all DOE Headquarters and field elements, including Federal organizations (hereinafter referred to as DOE elements).
  - b. This Notice applies to all DOE contractors. Contractor requirements pertaining to the Unclassified Cyber Security Program are listed in the Contractor Requirements Document (CRD), Attachment 1.
  - c. In this Notice, DOE elements and DOE contractors are collectively referred to as DOE organizations.
- 4. REQUIREMENTS.
  - a. Implementation.
    - (1) This Notice must be implemented by all DOE organizations no later than 180 days after issuance, throughout the Department, by means of contract or financial assistance agreements, specific performance criteria, and a performance measurement system. For DOE organizations not managed by a contractor, implementation must occur upon completion of accepted performance measures determined by agreement with the CIO. Extensions to the 180-day limit will be determined on a case-by-case basis by the CIO.
    - (2) Additional performance measures may be required for the following specific categories of unclassified information:
      - Unclassified Controlled Nuclear Information (UCNI),
      - Naval Nuclear Propulsion Information (NNPI),
      - Privacy Act Information,



- Export Controlled Information, and
  - Information marked “Official Use Only (OUO).”
- b. Cyber Resource Protection. Each DOE organization must ensure that all DOE unclassified information resources under its purview are protected in a manner that is consistent with its threats and missions at all times.
- c. Risk Management. DOE organizations must use a risk-based approach to identify information resources. A documented risk assessment process must be used to make informed decisions related to the adequacy of protection, cost implications of further enhanced protection, and acceptance of residual risk.
- d. Protection of Non-DOE Information. All DOE organizations must protect the information and information technology resources of other Federal Departments and agencies, State and local governments, and entities in the public sector.
- e. Resources. In coordination with the respective Lead Program Secretarial Officer (LPSO) and other Headquarters organizations, each DOE organization must plan, budget, allocate, and execute resources sufficient to ensure comprehensive implementation and maintenance of that organization’s computer security program.
- f. Cyber Security Program Plan. Each DOE organization must document its Cyber Security Program in a Cyber Security Program Plan (CSPP). The CSPP must be approved by the DOE organization’s operations, field office, or responsible Headquarters Organization manager following consultation with the DOE Lead Program Secretarial Office (LPSO), Office of the Chief Information Officer (CIO), and the Office of Independent Oversight and Performance Assurance (Independent Oversight). Normally, within 30 days of receiving it, the CIO and Independent Oversight will approve the proposed CSPP or suggest revisions. DOE organizations may revise their CSPPs as required by new operational considerations, risks, vulnerabilities, etc. DOE organizations must submit the revised CSPP to the organization’s operations, field office, or responsible HQ organization manager for approval. In urgent situations, they may anticipate approval and implement these revisions while waiting for formal approval.

If an organization is not under the purview of an operations or field office manager, the responsible DOE Headquarters organization must approve the CSPP. The DOE operations, field office, or responsible HQ organization manager is responsible for disposition of the approved CSPP, including submitting a copy of it to the Office of the CIO, which must maintain a current copy of each organization’s CSPP. Each DOE organization must provide copies of the draft and approved CSPP to Independent Oversight. At the request of the Office of the CIO, the Independent Oversight will review selected draft plans and provide informal comments on them to the Office of the CIO and to the organization’s operations, field office, or HQ responsible organization manager.

- g. CSPP Assessment and Review. To ensure that the CSPP is properly implemented, the following three-level review process is used.
- (1) Organization Self-Assessment. As called for by the CSPP, but no less frequently than once every 2 years, each DOE organization must evaluate its conformance with the approved CSPP. The evaluation must include a threat and risk assessment and a vulnerability analysis of the information systems identified in the organization's CSPP. The evaluation must also describe the residual risk accepted by the DOE organization manager. If the DOE organization manager is a contractor, the results of the evaluation must also be provided to the operations/field office manager, who is jointly responsible for accepting the residual risk. The DOE organization manager and the operations or field office manager may delegate formal acceptance of the risk, but they retain ultimate responsibility for security of the information systems and the information processed in the systems.
  - (2) Peer Review. At least once every 3 years, a peer organization must evaluate each DOE organization's CSPP and that organization's conformance with its CSPP. The results must be provided to the DOE organization manager and the Office of the CIO, and in those cases where the DOE organization manager is a contractor, the results must also be provided to the operations or field office manager. Peer reviews may be combined with self-assessments at the discretion of the DOE organization.
  - (3) Oversight review: Independent Oversight shall maintain a continuous program of independent oversight for cyber security. The independent oversight program will include announced and unannounced cyber security inspections, followup reviews, remote testing for network vulnerabilities (network scanning), and penetration testing. These reviews will assess the effectiveness of the cyber security protection program in meeting the requirements and intent of this directive and the organization's CSPP. Independent Oversight shall notify the cognizant DOE organization manager, LPSO, CIO, Office of Counterintelligence, and where applicable, the operations/field office manager of announced inspections. Independent Oversight will inform the Office of the CIO, Office of Counterintelligence, and the Computer Incident Advisory Capability prior to performing penetration testing on any site's computer systems. Results of each Independent Oversight review shall be provided to the same individuals and may include ratings of program effectiveness and issues requiring development and implementation of corrective action plans.
- h. Corrective Action Plans. Each DOE organization must draft and implement corrective action plans to address security shortfalls uncovered as a result of the oversight review process. The corrective action plans must include actions to be taken, responsible organizations and individuals for each action, the schedule (including key milestones), actions to address root causes and generic applicability, a process for tracking actions to closure, and steps to verify effectiveness of actions prior to closure.

7-26-99

- i. CIO Groups. To ensure that DOE policy and guidance are appropriate and current, two DOE cyber security groups must be established: the Technical Review Group and the Policy Planning Group. These groups will assist the CIO in developing guidance and recommended approaches for individual DOE organizations and DOE Program Secretarial Offices (PSOs) to use in fulfilling their respective responsibilities for ensuring adequate protection of DOE information resources. Both groups must be selected by the Office of the CIO, following a CIO-determined nomination process, and will be chaired by the Office of the CIO.
  - (1) The Technical Review Group must, on a continuing basis, assess technology issues, ascertain best security practices, and evaluate the changing nature of threats facing DOE and its organizations. The Technical Review Group will include representatives from DOE, its contractors, and other non-governmental participants who can provide the necessary technical insight and guidance.
  - (2) The Policy Planning Group must provide policy and best practice recommendations to the CIO. Its members will be drawn from throughout the DOE, including both Federal and contractor personnel.
- j. User Authentication. DOE organizations must employ user authentication techniques before allowing users to access systems that support multiple user accounts or that contain hard-to-replace or sensitive data. The organization's CSPP must indicate the systems or enclaves that require authentication and the type of authentication that must be employed.
- k. Access Protection. Access to a DOE organization's information resources must be protected commensurate with the risks and threats of its environment. The CSPP must specify the information resources to be protected and the protective mechanisms to be used.
- l. Auditing. DOE organizations must be capable of recording, and maintaining in an audit trail, information regarding access to and modifications of all information resources, where this is identified as appropriate by risk and vulnerability analysis, and such capability is technically feasible. The CSPP must state the systems or enclaves that must be audited, what information must be captured in that audit trail, and how long the audit trail must be maintained.
- m. Continuity of Service. DOE organizations must employ procedures and mechanisms to curtail or recover from activities that can disrupt or otherwise interfere with system availability, where operationally necessary and technically feasible. The CSPP must identify the organization's systems and enclaves that require such mechanisms and procedures and must detail the procedures and mechanisms employed.

- n. Security Monitoring. DOE organizations must report security incidents to the organization incident response team and to the Computer Incident Advisory Capability (CIAC). In addition, each DOE organization must provide 24-hour-a-day, 7-day-a-week coverage. The CSPP must specify the type of events that require monitoring, the enclaves and systems that will be subject to monitoring, how the 24x7 monitoring will be handled, and the composition of the organization incident response team. DOE organizations must also provide security incident information to the National Infrastructure Protection Center (NIPC) and the DOE Office of Counterintelligence as necessary, in accordance with all agreements.
- o. Response. DOE and contractor personnel must respond to CIAC cyber security advisories, bulletins, alerts, and suspected incidents in accordance with the policy and procedures stated in the organization's CSPP. The specific response must be commensurate with the perceived level of risk and may include containment, remediation, and increased monitoring. DOE organizations must coordinate joint responsive activities, and the CIO must direct responsive activities throughout DOE, as circumstances warrant.
- p. Training. Personnel from all DOE organizations and contractors must be appropriately trained in cyber security vulnerabilities, threats, protection strategies, and respective organizational and personal responsibilities. The CSPP must specify the details of the training program.
- q. Malicious Code. Each DOE organization must establish procedures and mechanisms, consistent with the threat environment, to limit (as technically feasible) the introduction of malicious code into its information systems. The CSPP must specify the mechanisms used to detect and prevent the installation of malicious code and the frequency of updating such mechanisms.
- r. Mission Interoperability Clusters. To facilitate consistency of security implementation among the DOE organizations, five specific mission interoperability clusters have been defined (see definition in Attachment 2). The CSPP must specify the mission interoperability clusters applicable to its mission and environment.
- s. Protection of Classified Information. Classified information must not be entered into unclassified information systems.
- t. Major Applications. For major Departmental applications where there is significant risk and where the application resides at multiple sites, it must be determined if a separate Computer Security Program and Computer Security Program Plan must be developed and implemented. The responsible LPSO, in coordination with the CIO, will be responsible for identifying Major Departmental Applications which require a separate Computer Security Program.

- u. CSPP Contents. The CSPP for each DOE organization must detail the approach to ensuring effective cyber security. The CSPP must account for the organization's specific environment, missions, and threats. At a minimum, each CSPP must be developed in accordance with all applicable policies, manuals and memorandums and address the following aspects of security.
  - (1) Define and assign cyber security roles and responsibilities.
  - (2) Define and describe cyber boundaries and boundary protection techniques, including the scope, specific security policies, connections external to an organization or identified enclave, and protection mechanisms required.
  - (3) Describe configuration management policies and practices, including a description of the process for making significant changes to the information system architecture and the organization's definition of "significant changes."
  - (4) Describe the following:
    - (a) the policy and procedures for responding to incidents at the organization, enclave, or system level as appropriate and in coordination with the Computer Incident Advisory Capability, and reporting to OCI and the NIPC,
    - (b) the procedures for disseminating and responding to advisories and lessons learned that are forwarded by the CIO or CIAC or generated at the site, and
    - (c) the composition of the organization incident response team.
  - (5) Describe the type of changes in technology, threat environment, or other changes to the organization, enclave, or system environment and architecture that would require the CSPP to be updated prior to its normal 2-year cycle.
  - (6) Describe the cyber security controls (technical and non-technical) employed to ensure confidentiality, integrity, availability, and accountability as required to accommodate the specific threats identified for information entered, processed, stored, displayed, or transmitted. These include, but are not limited to, the following:
    - (a) Authentication: Describe the type of authentication mechanisms employed, identify the systems and enclaves that require authentication, and, for those systems and enclaves that do not require user authentication, provide a rationale for said decisions.
    - (b) Access Protection: Describe the access control processes and procedures employed at the DOE organization, which include, but are not limited to–

- 1 identification of those information systems that require isolation or protection;
  - 2 a summary of strategy for securely accessing enclaves from locations outside of the enclave (including locations both inside and outside of the DOE organization); and
  - 3 a description of circumstances under which penetration testing may be used to validate access protection mechanisms.
- (c) Audit: Specify the enclaves, systems, and services (including email) that will be subject to auditing, what information must be collected, and how long audit information must be maintained.
- (d) Security Monitoring: Describe the type of events for which monitoring must be employed, which enclaves, clusters, and systems are subject to monitoring, and how 24x7 monitoring must be handled.
- (e) Continuity of Service: Identify those enclaves and systems that, due to mission operation necessities, have a low tolerance for disruption or unavailability; describe the procedures and mechanisms that will be employed to limit (as technically feasible) and recover from such disruption or unavailability.
- (7) Describe the process for ascertaining the current operational threat, risk, and vulnerability posture; the description must specify:
  - (a) who (by title/position) within the organization conducts the threat, risk, and vulnerability assessments;
  - (b) how such threat, risk, and vulnerability assessments are to be conducted; and
  - (c) how frequently such assessments must be conducted.
- (8) Describe the methodology being used for training (e.g., briefings, email), specify how frequently re-training should occur, identify those positions requiring training, and identify (by title/position) those responsible for overseeing training activities at the contractor's organization.
- (9) Describe the approach employed to address malicious code (e.g., handled at boundary, handled at desktops, and handled at selected locations), the mechanisms employed, and frequency of updating anti-malicious code software.

- (10) Describe the metrics employed to assess compliance with the CSPP and the process for evolving these metrics.
- (11) Describe the process for selecting peer members to review the contractor's CSPP and its compliance with the CSPP. The description should include qualifications required of the prospective individuals or entities and who makes the selection.
- (12) Identify those mission interoperability clusters that apply to the DOE organization.
- (13) Identify the DOE organization manager by title or position.

5. RESPONSIBILITIES.

a. Chief Information Officer (CIO).

- (1) Develops Departmental cyber security policies and guidance.
- (2) Maintains DOE-wide cognizance of cyber security resources.
- (3) Advocates cyber security funding, as appropriate.
- (4) Directs DOE-wide activities in response to cyber incidents in coordination with OCI, as circumstances warrant.
- (5) Reviews selected CSPPs.
- (6) Coordinates with the LPSOs to monitor implementation of DOE cyber security programs.
- (7) Coordinates with the LPSOs to facilitate establishment and implementation of needed DOE-wide technical security interoperability standards.
- (8) Coordinates with the LPSOs to develop program-specific cyber security policies, guidance, and procedures.
- (9) Coordinates with CIAC, the LPSOs, and the Office of Counterintelligence in establishing DOE incident reporting policy and standards.
- (10) At the CIO's discretion, participates in Independent Oversight-scheduled inspections and assessments to collect information that may be useful in developing or modifying policies and guidelines.

- (11) Defines a nomination and selection process for Technical Review Group and Policy Planning Group membership.
  - (12) Chairs the Technical Review Group and the Policy Planning Group.
  - (13) Establishes cyber security education, training, and awareness efforts throughout the DOE.
  - (14) Provides training information and material on DOE-wide cyber security threats, protection strategies, and organizational responsibilities.
- b. Lead Program Secretarial Officers (LPSO).
- (1) Coordinate with the CIO on 5a(5-7).
  - (2) Are responsible and accountable for cyber security of information resources under the purview of their respective programs.
  - (3) Ensure that adequate resources are budgeted and allocated to implement cyber security for their respective programs.
  - (4) Ensure that program roles and responsibilities for cyber security are clearly defined. The LPSO will ensure that a single, senior-level individual is designated as the focal point for cyber security in the headquarters, the field and operations offices, and each site as appropriate.
  - (5) Ensure that each DOE organization within their cognizance has an approved CSPP.
  - (6) Monitor the effectiveness of cyber security of unclassified National Security, Management and Administration, and Business Operations information through program reviews, self assessments, management assessments, performance metric results, and Independent Oversight evaluations; LPSOs may designate a representative to observe scheduled inspections and assessments conducted by Independent Oversight.
  - (7) Cooperate fully with external and internal review and oversight organizations, including Independent Oversight.
  - (8) In response to issues identified by Independent Oversight, develop corrective action plans within 60 days.



c. Line Managers Responsible for DOE Organization Cyber Security.<sup>1</sup>

- (1) Assume responsibility and accountability for their organizations' cyber security programs.
- (2) Ensure that adequate resources are allocated to the organization's Cyber Security Program.
- (3) Ensure that organization roles and responsibilities for cyber security are clearly defined.
- (4) Appoint a single individual responsible for all aspects of an organization's cyber security, such as an organization CIO or equivalent.
- (5) Monitor the effectiveness of cyber security through self assessments and reviews.
- (6) Assume responsibility for accepting residual risk.
- (7) Cooperate fully with external and internal review and oversight organizations, including Independent Oversight.
- (8) In response to issues identified by Independent Oversight, develop corrective action plans within 60 days.

d. Operations Office or Field Office Manager.

- (1) Approves the organization CSPP.
- (2) Shares responsibility for accepting residual risk when the DOE organization manager is a contractor.

e. The Office of Oversight and Performance Assurance (Independent Oversight).

- (1) Designs and implements an independent oversight program that encompasses DOE cyber security policy and implementation of that policy at DOE organizations.
- (2) As the sole focal point for DOE Headquarters oversight, periodically evaluates cyber security programs at DOE organizations. Such evaluations may include scheduled onsite inspections, unannounced inspections, remote scanning, penetration testing, and other such techniques.

---

<sup>1</sup> These individuals might be Laboratory directors, operations or field office managers, or responsible Headquarters managers.

- (3) Develops inspection methods and tools for evaluating cyber security.
  - (4) Identifies and tracks issues identified during independent oversight activities.
  - (5) Recommends improvements for the Unclassified Cyber Security Program to the organizations, LPSOs, and CIO.
  - (6) Reviews selected Cyber Security Program Plans.
  - (7) Evaluates and rates the effectiveness or performance of DOE organizations in meeting the requirements and intent of cyber security policy.
  - (8) Solicits input from the CIO and Office of Counterintelligence on inspection topics of concern for scheduled inspections; notifies the CIO, Office of Counterintelligence, and LPSO of scheduled inspections and provides an opportunity to participate.
  - (9) Analyzes the effectiveness of and trends in Departmental cyber security.
  - (10) Cooperates with the CIO, LPSOs, DOE organization managers, and the Office of Counterintelligence to identify potential solutions to DOE-wide or high-priority DOE organization-specific problems, in a manner that does not compromise the independence of Independent Oversight.
- f. DOE Computer Incident Advisory Capability (CIAC).
- (1) Serves as the DOE central computer incident reporting and analysis capability.
  - (2) Assists DOE organizations as requested in dealing with incidents and in performing assistance reviews.
  - (3) Advises DOE organizations of cyber security incidents, threats, and vulnerabilities and provides a watch and warning capability for the Department.
  - (4) Analyzes incidents reported by organizations, prepares summary reports of the incident information, and provides these reports to line managers responsible for element cyber security, LPSOs, the CIO, and Independent Oversight.
- g. Office of Counterintelligence.
- (1) Coordinate with DOE elements, PSOs, the CIO and other policy and technical planning bodies in defining policy, identifying data and technical requirements, and implementing initiatives to meet CI needs and purposes.

- (2) Conduct CI analysis of intrusion activity occurring across DOE sites.
  - (3) In coordination with CIO, OCI will coordinate the investigation of intrusions into the DOE systems with DOE field elements and NIPC until such time as it is determined that the intrusion is not a CI problem.
  - (4) OCI will perform independent inspections of CI programs at DOE facilities, to include evaluation of security components which impact the CI program, in coordination with Independent Oversight.
  - (5) In coordination with Independent Oversight, conduct vulnerability analyses and Red Teaming.
6. CONTACT. To provide comments and obtain assistance concerning this order, contact the Office of the Chief Information Officer at (202) 586-0166.
7. REFERENCES.
  - a. Clinger-Cohen Act of 1996. Public Law 104-106, which requires agencies to establish an information technology architecture.
  - b. National Technology Transfer and Advancement Act of 1995. Public Law 104-113, which supports Federal involvement in voluntary standards bodies.
  - c. Office of Management and Budget (OMB) Memorandum, June 18, 1997. A memorandum that concerns information technology architectures and calls for a technical reference model and standards profiles.
  - d. OMB Circular A-119. "Federal Participation in the Development and Use of Voluntary Standards."
8. DEFINITIONS. Attachment 2 contains a listing of definitions specific to the DOE Unclassified Cyber Security Program.

BY ORDER OF THE SECRETARY OF ENERGY:



JOHN M. GILLIGAN  
CHIEF INFORMATION OFFICER

## **CONTRACTOR REQUIREMENTS DOCUMENT**

1. **CYBER RESOURCE PROTECTION.** Each DOE contractor must ensure that all DOE unclassified information and information systems under its purview are protected in a manner that is consistent with its threats and missions at all times.
2. **RISK MANAGEMENT.** Each DOE contractor must use a risk-based approach to protect information and information systems. A documented risk assessment process must be used to make informed decisions related to the adequacy of protection, cost implications of further enhanced protection, and acceptance of residual risk.
3. **PROTECTION OF NON-DOE INFORMATION.** Each DOE contractor must protect the information and information technology resources of other Federal Departments and agencies, State and local governments, and entities in the public sector.
4. **CYBER SECURITY PROGRAM PLAN.** Each DOE contractor must document its Cyber Security Protection Program in a Cyber Security Program Plan (CSPP). The CSPP must be approved by the DOE Office of the Chief Information Officer (CIO) and the Office of Independent Oversight and Performance Assurance (Independent Oversight). Contractors may revise their CSPPs as required by new operational considerations, risks, vulnerabilities, etc. Contractors must submit these revisions to their operations or field office manager. In urgent situations, they may anticipate approval and implement these revisions while waiting for formal approval.
5. **CSPP ASSESSMENT AND REVIEW.** To ensure that the CSPP is properly implemented, the contractor must ensure that the following three-level review process is used.
  - a. **Organization Self-Assessment.** As called for by the CSPP, but no less frequently than once every 2 years, each DOE contractor must evaluate its conformance with the approved CSPP. The evaluation must include a threat and risk assessment and a vulnerability analysis of its information systems. The evaluation must also describe the residual risk accepted by the contractor, including a listing of any waivers from the policy mandated by either the CSPP or DOE.
  - b. **Peer Review.** At least once every 3 years, a peer organization must evaluate each DOE contractor's conformance with the approved CSPP. The results must be provided to the cognizant Federal line manager, DOE organization manager (e.g., lab director), operations/field office manager, and the Office of the CIO.
  - c. **Oversight Review.** An oversight review must be performed on each DOE contractor's Unclassified Cyber Security Program to assess its conformance with the approved CSPP.

These reviews will assess effectiveness of the cyber security protection program in meeting the requirements and intent of this directive and the contractor's CSPP. Independent Oversight will notify the DOE contractor, LPSO, CIO, Office of Counterintelligence, and the operations/field office manager of scheduled inspections, so they may participate. Results of each Independent Oversight review will be provided to the same individuals and may include ratings of program effectiveness and issues requiring development and implementation of corrective action plans.

6. CORRECTIVE ACTION PLANS. Each DOE contractor must draft and implement corrective action plans to address security shortfalls uncovered as a result of the oversight review process. The corrective action plans must include actions to be taken, responsible organizations and individuals for each action, schedule including key milestones, actions to address root causes and generic applicability, tracking of actions to closure, and steps to verify effectiveness of actions prior to closure.
7. THE SECURITY POLICY PLANNING GROUP. DOE contractors must provide representatives to this group as requested by DOE.
8. USER AUTHENTICATION. DOE contractors must employ user authentication techniques before allowing users to access systems that support multiple user accounts or systems that contain restricted, hard-to-replace, or sensitive data. The CSPP must indicate the systems or enclaves that require positive authentication and the type of authentication that must be employed.
9. ACCESS PROTECTION. Each DOE contractor must protect its information and information systems as specified in the CSPP. The CSPP must specify the information and systems to be protected and the protective mechanisms to be used.
10. AUDITING. Each DOE contractor must be capable of recording, and maintaining in an audit trail, information regarding access to and modifications of all information resources, where this is identified as appropriate by risk and vulnerability analysis, and such capability is technically feasible. The CSPP must state the systems or enclaves that must be audited, what information must be captured in that audit trail, and how long the audit trail must be maintained.
11. CONTINUITY OF SERVICE. DOE contractors must employ procedures and mechanisms to curtail or recover from activities that can disrupt or otherwise interfere with system availability, where operationally necessary and technically feasible. The CSPP must identify the contractor's systems and enclaves that require such mechanisms and procedures and must detail the procedures and mechanisms employed.

12. SECURITY MONITORING. Each DOE contractor must report security incidents to their site incident response team and to the Computer Incident Advisory Capability (CIAC). In addition, each DOE contractor must provide 24-hour-a-day, 7-day-a-week coverage. The CSPP must specify the type of events that require monitoring, the enclaves and systems that will be subject to monitoring, how the 24x7 monitoring will be handled, and the composition of the organization incident response team. DOE contractors must also provide security incident information to the National Infrastructure Protection Center (NIPC) and the DOE Office of Counterintelligence as necessary, in accordance with all agreements.
13. CYBER SECURITY ADVISORIES, ALERTS, AND SUSPECTED INCIDENTS. Contractor personnel must respond to CIAC cyber security advisories, bulletins, alerts, and suspected incidents in accordance with the policy and procedures stated in the organization's CSPP. The specific response must be commensurate with the perceived level of risk and may include containment, remediation, and increased monitoring.
14. TRAINING. All DOE contractor personnel must be appropriately trained in cyber security vulnerabilities, threats, protection strategies, and respective organizational and personal responsibilities. The CSPP must specify the details of the training program.
15. MALICIOUS CODE. Each DOE contractor must establish procedures and mechanisms, consistent with the threat environment, to limit (as technically feasible) the introduction of malicious code into its information systems. The CSPP must specify the mechanisms used to detect and prevent the installation of malicious code and the frequency of updating such mechanisms.
16. MISSION INTEROPERABILITY CLUSTERS. To facilitate consistency of security implementation among the DOE organizations, five specific mission interoperability clusters have been defined. In its CSPP, the contractor must specify the mission interoperability clusters applicable to its mission and environment.
17. CSPP CONTENTS. The CSPP for each DOE contractor must detail the approach to ensuring effective cyber security. The CSPP must account for the contractor's specific environment, missions, and threats. At a minimum, the CSPP must address the following aspects of security.
  - a. Define and assign cyber security roles and responsibilities.
  - b. Define and describe cyber boundaries and boundary protection techniques, including the scope, specific security policies, connections external to an organization or identified enclave, and protection mechanisms required.

- c. Describe configuration management policies and practices, including a description of the process for making significant changes to the information system architecture and the contractor organization's definition of "significant changes."
- d. Describe the procedures for responding to incidents at the organization, enclave, or system level as appropriate and in coordination with the Computer Incident Advisory Capability.
- e. Describe the type of changes in technology, threat environment, or other changes to the organization, enclave, or system environment and architecture that would require the CSPP to be updated prior to its normal 2-year cycle.
- f. Describe the cyber security controls (technical and non-technical) employed to ensure confidentiality, integrity, availability, and accountability as required to accommodate the specific threats identified for information entered, processed, stored, displayed, or transmitted. These include, but are not limited to, the following:
  - (1) Authentication: Describe the type of authentication mechanisms employed, identify the systems and enclaves that require positive authentication, and, for those systems and enclaves that do not require positive user authentication, provide a rationale for said decisions.
  - (2) Access Protection: Describe the access control process and procedure employed at the DOE organization, which include, but are not limited to—
    - (a) identification of those information systems that require isolation or protection;
    - (b) summary of strategy for securely accessing enclaves from locations outside of the enclave (including locations both inside and outside of the DOE organization); and
    - (c) a description of circumstances under which penetration testing may be used to validate access protection mechanisms.
  - (3) Audit: Specify the enclaves, systems, and services (including email) that will be subject to auditing, what information must be collected, and how long audit information must be maintained.
  - (4) Security Monitoring: Describe the type of events for which monitoring must be employed, which enclaves, clusters, and systems are subject to monitoring, and how 24x7 monitoring will be handled.

- (5) Denial of Service: Identify those enclaves and systems that, due to mission operation necessities, have a low tolerance for disruption or unavailability; describe the procedures and mechanisms that will be employed to limit (as technically feasible) and recover from such disruption or unavailability.
- g. Describe the process for ascertaining the current operational threat, risk, and vulnerability posture; the description must specify–
  - (1) who (by title/position) within the organization conducts the threat, risk, and vulnerability assessments;
  - (2) how such threat, risk, and vulnerability assessments are to be conducted; and
  - (3) how frequently such assessments must be conducted.
- h. Describe the methodology being used for training (e.g., briefings, email), specify how frequently re-training should occur, identify those positions requiring training, and identify (by title/position) those responsible for overseeing training activities at the contractor's organization.
- i. Describe the approach employed to address malicious code (e.g., handled at boundary, handled at desktops, handled at selected locations), the mechanisms employed, and frequency of updating anti-malicious code software.
- j. Describe the metrics employed to assess compliance with the CSPP and the process for evolving these metrics.
- k. Describe the process for selecting peer members to review the contractor's CSPP and its compliance with the CSPP. The description should include qualifications required of the prospective individuals or entities and who makes the selection.
- l. Identify those mission interoperability clusters that are applicable to the DOE contractor's organization.
- m. Identify (by title/position) the DOE contractor's organization manager.



## **DEFINITIONS**

The following terms are specific to the DOE Unclassified Cyber Security Program. Some definitions include a citation indicating the source. Citations are given in full on first use and are abbreviated thereafter. Where no citation appears, the term has been derived from several sources or from common usage. Many definitions are from the National Security Telecommunications and Information Systems Security Committee's *National Information Systems Security (INFOSEC) Glossary*. Other definitions may be found in the *DOE Glossary*, which is available online.

**ACADEMIC RESEARCH/SCIENCE OPERATIONS.** The mission interoperability cluster dealing with information used for academic research and for operating science facilities.

**AUDIT TRAIL.** A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. [National Computer Security Center, *Glossary of Computer Security Terms*, 21 October 1988.]

**AUTHENTICATION.** Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [National Security Telecommunications and Information Systems Security Committee. *National Information Systems Security (INFOSEC) Glossary*. NSTISSI No. 4009, August 1997. Hereafter cited as "NSTISSI 4009."]

**COMPUTER INCIDENT ADVISORY CAPABILITY (CIAC).** The Department-wide computer network incident response capability; a dedicated capability to monitor, analyze, track, summarize, and report cyber security incidents, and to issue alerts and advisories.

**COMPUTER NETWORK.** An interconnected collection of autonomous computers. [DOE Glossary]

**CONFIGURATION MANAGEMENT.** Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system. [NSTISSI 4009.]

**CONTAINMENT.** Ensuring that neither attacks nor responses result in severe and undesirable damage, either to operational capabilities, to any personnel, or to equipment or property of any kind.

**CONTRACTOR.** See DOE contractor.

**COUNTERMEASURE.** Anything that effectively negates an intruder's ability to exploit vulnerabilities.

CYBER SECURITY. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, against loss of accountability for information and user actions, and against the denial of service to authorized users, including those measures necessary to protect against, detect, and counter such threats.

DENIAL OF SERVICE. Result of any action or series of actions that prevents any part of an information system from functioning. [NSTISSI 4009.]

DEPARTMENTAL ELEMENTS. First-tier organizations at Headquarters and in the field. First-tier entities at Headquarters are the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and Staff Office Directors). First-tier entities in the field are Managers of the eight operations offices, managers of the three field offices, and the administrators of the power marketing administrations. Headquarters and field elements are described as follows:

1. Headquarters elements are DOE organizations located in the Washington metropolitan area.
2. "Field elements" is a general term for all DOE elements (excluding individual duty stations) located outside of the Washington, DC, metropolitan area. [DOE Glossary]

DOE CONTRACTOR. An entity who receives an award from DOE, including management and operating contractors, which manage, operate, or provide DOE element services to DOE research or production facilities that are principally engaged in work for the DOE. [DOE Glossary]

DOE ORGANIZATION. A Department Headquarters element or field element that includes both DOE Federal and DOE contractor entities.

DOE ORGANIZATION MANAGER. The Federal employee or contractor who heads a DOE organization.

ENCLAVE. A set of information and processing capabilities that are protected as a group.

EXPORT CONTROLLED INFORMATION. Certain unclassified Federal Government information under DOE's cognizance that, if generated by the private sector, would require a specific license or authorization for export under U.S. laws or regulations. [DOE Glossary]

FIELD ELEMENT. See Departmental element. [DOE Glossary]

GOVERNMENT INFORMATION. Information created, collected, processed, disseminated, or disposed of by or for the Federal Government. [DOE Glossary]

**INCIDENT.** Any adverse event that threatens the security of information resources. Adverse events include compromises of integrity, denial of service, compromises of confidentiality, loss of accountability, or damage to any part of the system. Examples of incidents include the insertion of malicious code (e.g., viruses, Trojan horses, or backdoors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.

**INDUSTRY/OTHER (NON-NATIONAL SECURITY/ACADEMIC) GOVERNMENT RESEARCH.** The mission interoperability cluster dealing with information and functions, such as Cooperative Research and Development Agreements (CRADAs), “work for others,” proprietary information trade agreements, and industrial/commercial collaborative research.

**INFORMATION.** Any communication or reception of knowledge such as facts, data, or opinions including textual, numerical, graphic, cartographic, narrative, or audiovisual forms, whether oral or maintained in any medium, including computerized databases, paper, microform, or magnetic tape. [DOE Glossary]

**INFORMATION RESOURCES.** Information, information technology, and information systems.

**INFORMATION SYSTEM.** A discrete set of information and information technology organized to collect, process, maintain, transmit, and disseminate information, in accordance with defined procedures, whether automated or manual.

**INTEROPERABILITY.** The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and use the services so exchanged to enable them to operate together. [DOE Glossary]

**INTEROPERABILITY STANDARD.** A document that establishes engineering and technical requirements necessary to be employed in the design of systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. [DOE Glossary]

**INTRUSION.** An unauthorized access to an information resource.

**INTRUSION DETECTION.** The logging and auditing capability that provides evidence that an attempt or actual breach of protection mechanisms or access controls has occurred.

**LEAD PROGRAM SECRETARIAL OFFICER.** See secretarial officer.

**MAJOR APPLICATION.** An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note; All Federal applications require some level of protection. Certain applications, because of the information in them; however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Source: Appendix III to OMB Circular No. A-130)

MANAGEMENT/ADMINISTRATIVE/BUSINESS OPERATIONS. The mission interoperability cluster that deals with such functions as personal dosimetry reports, contractor performance appraisals (including fees and penalties data), personnel data, other-than-science facility operations, production operations, grants and proposal administration, and procurement data. DOE contractor systems that are incidental to the contract in this cluster are the sole responsibility of the contractor.

MISSION INTEROPERABILITY CLUSTER (MIC). Information resources performing similar functions within DOE that use data of similar sensitivity levels, and that have similar computer security concerns and protection requirements across all DOE organizations.

The five specific mission interoperability clusters are listed below.

1. **Unclassified National Security/Nuclear:** Information that is unclassified but still requires protection, such as Unclassified Controlled Nuclear Information (UCNI), export-controlled information (ECI), and Naval Nuclear Propulsion Information (NNPI).
2. **Management, Administration, Business Operations:** Information that is unclassified but still requires protection, such as proprietary information (but not third-party proprietary), Privacy Act, and the majority of the exemptions to the Freedom of Information Act ("Official Use Only" information).
3. **Industry and Other Government Research:** Information that is unclassified but still requires protection, such as third-party proprietary information, Protected CRADA (Cooperative Research and Development Agreement) Information, and other information protected by its sponsor (such as "technical data" from the Department of Defense).
4. **Academic Research, Scientific Operations:** Information that is unclassified but is considered sensitive because it is in "pre-publication" form and is not appropriate for general release; it may or may not require special protection.
5. **Open, Public, Unrestricted:** Information that requires no protection from disclosure.

MONITORING. Near-real-time collection and analysis of information about system behavior, such as throughput or performance, which could indicate a security incident.

OFFICIAL USE ONLY.

1. A designation identifying certain unclassified but sensitive information that may be exempt from public release under the Freedom of Information Act or
2. a former (7-18-49 through 10-22-51) security classification marking. [DOE Glossary]

OPEN/PUBLIC/UNRESTRICTED. The mission interoperability cluster dealing with information provided for public access.

OVERSIGHT. Refers to the responsibility and authority assigned to the Assistant Secretary for Environment, Safety and Health to independently assess the adequacy of DOE and contractor performance. Oversight is separate and distinct from line management activities, including self-assessments. [DOE Glossary]

PERFORMANCE MEASURE. A process of assessing progress toward achieving predetermined goals. [DOE Glossary]

PROGRAM OFFICE. A Headquarters organization that is responsible for executing program management functions, and which is responsible for assisting and supporting field elements in safety and health, administrative, management, and technical areas. [DOE Glossary]

PROGRAM SECRETARIAL OFFICER. See secretarial officer. [DOE Glossary]

REMEDIATION. Recovery of functional capabilities; restoration of the integrity of data and software; removal of malicious code, data, and devices; and repair of physical damage.

RESEARCH. A systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to general knowledge. Activities that meet this definition constitute “research” for purposes of protecting human subjects, whether or not they are conducted under a program considered research for other purposes (i.e., some “demonstration” and “service” programs may include research activities). [DOE Glossary]

RESPONSIVE ACTIVITIES. Activities taken in response to a cyber security advisory, alert, or suspected incident, including containment, reporting, monitoring and observation, remediation, retaliation (e.g., legal action), and presentation of information to the public or to other organizations.

RESIDUAL RISK. The portion of risk remaining after security measures have been applied. [NSTISSI 4009.]

RISK. The probability that an undesired result or event such as theft, loss, damage, or injury will occur. Exposure to the chance of loss, damage, or injury. [DOE Glossary]

SAFEGUARDS AND SECURITY INTEREST. A general term for any DOE asset, resource, or property that requires protection from malevolent acts. It may include but is not limited to classified matter, special nuclear material and other nuclear materials, secure communications centers, sensitive compartmented information facilities, automated data processing centers, facilities storing and transmitting classified information, vital equipment, or other DOE property. [DOE Glossary]

SECRETARIAL OFFICER. Secretarial Officers are the Secretary, Deputy Secretary, and Under Secretary; and the Assistant Secretaries and Staff Office Directors reporting to the Secretary either directly or through the Deputy Secretary or Under Secretary. The following designations are also used to identify Secretarial Officers with specific responsibilities in various areas.

1. A Program Secretarial Officer is a Head of a Departmental element who has responsibility for a specific program or facility(ies). These include the Assistant Secretaries for Defense Programs, Energy Efficiency and Renewable Energy, Environmental Management, and Fossil Energy; and the Directors of the Offices of Civilian Radioactive Waste Management, Science, and Nuclear Energy.
2. A Cognizant Secretarial Officer is a DOE official at the Assistant Secretary level who is responsible for the assignment of work, the institutional overview of any type of facility, or both, and the management oversight of a laboratory. [DOE Glossary]

THREAT. Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NSTISSI 4009.]

TRAINING. The process of providing for and making available to an employee(s) and placing or enrolling an employee(s) in a planned, prepared, and coordinated program, course, curriculum, subject, system, or routine of instruction or education, in fiscal, administrative, management, individual development, or other fields that improve individual and organizational performance and assist in achieving the agency's mission and performance goals. [DOE Glossary]

UNCLASSIFIED. The designation for information, a document, or material that has been determined not to be classified or that has been declassified by proper authority. [DOE Glossary]

UNCLASSIFIED NATIONAL SECURITY/NUCLEAR. The mission interoperability cluster dealing with unclassified information and systems related to national security. This MIC includes the following systems: Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), military/dual use information, nonproliferation information, and other sensitive, but not classified, information.

USER AUTHENTICATION. Reliable identification of users of an information system.

VIRUS. Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. [NSTISSI 4009.]

VULNERABILITY. A weakness or system susceptibility that if exploited would cause an undesired result or event leading to loss or damage, as follows:

1. Major Vulnerability is a vulnerability that, if detected and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security.
2. Unspecified Major Vulnerability is a major vulnerability, but specified in no greater detail than the specific security system (or one of its major components) when it occurs. A weakness in a system or organization's defenses that could be exploited. [DOE Glossary]

VULNERABILITY ANALYSIS. A systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a safeguards and security system to protect specific targets from specific adversaries and their acts. [DOE Glossary]

VULNERABILITY ASSESSMENT. See vulnerability analysis.